Christopher I. McIntosh

Statewide Interoperable Communications Coordinator

Office of Veterans Affairs and Homeland Security

Office of the Governor

Commonwealth of Virginia

September 12, 2012

Resilient Communications: Current Challenges and Future Advancements

Eleven years ago yesterday, interoperable communications was identified as one of the major areas of public safety that required major improvement following the attacks of 9/11. Communications is the one constant that forms the foundation for all other public safety disciplines; it is the bedrock of every response plan, the core of every procedure. Without reliable communications, effective command and control cannot be achieved, critical information cannot be passed, and life threatening developments cannot be shared. In the past eleven years, billions of dollars have been spent across the nation, new radio systems have been fielded, interoperability has been greatly improved, and the ability of our first responders, emergency mangers, and homeland security professionals to communicate is better than ever.

We stand at a crossroads, however. Many of those critical radio systems procured in the years following 9/11 are becoming antiquated. Technology, as is always the case, has continued its relentless advance resulting in the need to perform major upgrades to existing systems, or in some cases wholesale replacement. The increased use of the finite radio spectrum has resulted in the FCC requirement to "narrowband", resulting in improved efficiency in the use of radio spectrum, but also creating the de facto obsolescence of an entire generation of radio equipment. Maintenance and sustainment costs for existing systems alone cost hundreds of millions of dollars, forcing jurisdictions to make tough budgetary choices, often resulting in critical systems no longer being supported.

All of this is occurring while funding levels have fallen precipitously. Virginia has seen consecutive 50% cuts in State Homeland Security Grant Programs, dropping from $18M in 2010 to less than $5M in 2012. Historically, almost 30% of this funding has gone to support and maintain our communications programs. In 2011 alone, the Commonwealth received $43M in requests from localities for communications grant funding, and was only able to allocate $2M, resulting in many necessary projects going unfunded. Virginia has also seen the loss of two Urban Area Security Initiatives (UASIs). The loss of the Central Virginia and Hampton Roads UASIs resulted in the loss of tens of millions of dollars in annual funding. Systems implemented in those areas did not go away, however, and now must compete with the rest of the Commonwealth for the dwindling SHSGP funding stream while their costs are migrated to local budgets. The invaluable Interoperable Emergency Communications Grant Program

(IECGP) has also not been funded. This grant provided for the planning, training, and exercises that improved the capabilities of the most important component of any communications program, the people. Technology is useless without knowledgeable people who know how to use it properly, have identified and trained to its capabilities and limitations, and have planned and exercised its application in numerous settings. IECGP also funded many of the Statewide Interoperability Coordinators (SWICs) around the country, whose job it is to focus solely on the issues surrounding Interoperable Communications. Through the SWICs, states now have Statewide Interoperablility Executive Committees (SIECs) that pull people in from across jurisdictions and disciplines, allowing them to work together to solve cross cutting communications problems, share lessons learned and best practices, and write strategic plans that shape a common direction forward. With the loss of IECGP, these positions, and the associated governance structures, are beginning to fall victim to the budget axe.

Simultaneously, we stand on the verge of a revolution in emergency communications capabilities. Traditional Land Mobile Radio systems are beginning to become integrated with Voice over Internet Protocol (VoIP) technologies. By fusing voice communications with internet technologies, a whole new world of possibilities is becoming a reality. Virginia operates one of the largest Public Safety VoIP networks in the nation which, by the end of CY 2012, will have points of presence in 122 jurisdictions, as well as the Virginia State Police, Department of Transportation, and Department of Emergency Management. The Commonwealth's Link to Interoperable Communications (COMLINC) program allows different radio systems to be linked together, much in the way that other radio gateways do, resulting in interoperability through the creation of a "patch" by an operator in a Public Safety Answering Point (PSAP). The true potential of COMLINC, when fully implemented, lies in its VoIP functionality. Soon, any laptop, tablet, or smart phone in the hands of a public safety professional will become a radio capable of communicating with any PSAP in the state, or any responder on a radio connected to it.

Due to this advancement, interoperable communications no longer involves just voice and radio systems. We are entering an era where interoperable *information* is the goal. Advances in Computer Aided Dispatch (CAD), Crisis Management, VoIP, video, and Geospatial Information Systems (GIS) allow for the sharing and display of information that allows decision makers and responders to have previously unheard of levels of situational awareness. Using the common denominator of location, the ability to merge real-time information such as CAD, weather, sensor data, video, and Crisis Management reports with mapping systems and plan overlays allows personnel, from the tactical to the strategic, to have a better understanding of a given situation, presenting information in context that is critical for effective decision making. For example, a large hazmat on the highway is one thing, but a large hazmat on the highway upwind from a county fair in a neighboring jurisdiction is something else entirely. The integration of COMLINC and its VoIP functionality now allows not only the rapid understanding of the true severity of a situation, but also allows for the interaction of decision makers through the same interface. Potentially, the days of a journal full of usernames and passwords, hopping from system to system searching for tidbits of relevant information, will be a thing of the past. Virginia has recently completed a pilot project in the Charlottesville/Albermarle region that demonstrated that this is possible today. We are following that pilot up with another in Hampton Roads that kicks of this month, with the goal of realizing a statewide information sharing capability by the end of next year.

It is important to note that we are not doing this in a vacuum. Virginia along with Oregon and California initiated a National Information Sharing Consortium (Consortium) in order to share technology and best practices which will enable state and local agencies across the country to work in tandem towards these goals which we all share. Through the Consortium, which is growing daily, we will be able to leverage one another's experiences so that we, as a community, don't repeat costly mistakes over and over again. Additionally, we are also working closely with the DHS Science and Technology First Responders Group (FRG) and its Office of Interoperability and Compatibility (OIC) who are providing us critical assistance in assessing and working through the issues with the new generation of technologies that can facilitate achieving these goals such as shared services in "the cloud" and various "bridge" technologies. Taken together all of this will enable us to create a true "Virtual USA" enabling intrastate and interstate interoperability and will serve as the roadmap towards making use of the new broadband capabilities when they reach fruition.

All of these capabilities, indeed the entire path forward, rely on reliable connectivity. The events of the Derecho storm at the end of June 2012 demonstrate how vulnerable public safety networks, where they exist, are to saturation, degradation, or destruction. As the Derecho showed, the loss of a couple of key facilities can result in a cascading failure that affects millions of people's potential safety and security. In many cases, public safety responders rely on the public network for mission critical communications. This is especially true in the wireless world, where the rise in popularity of smart devices has created a demand for bandwidth that threatens to overwhelm the entire network when an incident occurs. According to the President's Council of Advisors on Science and Technology's report entitled "Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth", the amount of wireless data transmitted from smart phones and wirelessly connected tablets has doubled every year for the last four years. We saw this scenario realized during the recent earthquake in central Virginia. When the shaking stopped, most people picked up their phones to call a loved one, text a friend, or post on a social media site. This spike in volume resulted in the inability of the public safety community to communicate via wireless network, both with each other and with the public. Text message based alerting systems were rendered useless, as the networks that they are dependent upon were so overwhelmed by traffic that texts didn't get through for up to 30minutes, if at all. Phone calls were pointless, emails were spotty.

The problem isn't limited to the wireless world. We are increasingly reliant on the internet itself for communicating critical information. Everything from accessing the latest weather requesting assistance now flows on the web, the same web that you or I use at home. Bandwidth in the terrestrial network is a finite resource, subject to the similar loading demands as the wireless network. In Virginia, we experienced degradation in our capability to use web based information during several large scale events. During tropical storm Hanna, the prevalence of teleworkers in the Richmond area resulted in difficulty in obtaining critical weather information from the National Weather Service website. Ironically, my mom, at home in another part of the state, had no trouble whatsoever accessing the same information that I was struggling to get at the State EOC. Unfortunately, there is currently no way for public safety to prioritize traffic on the public internet.

Public Safety Broadband offers a solution that addresses many of the connectivity issues faced by public safety. Its advocates the needs of first responders and public safety professionals to have unfettered access to wireless communications in order to improve their ability to respond to incidents safely and effectively. I couldn't agree more, but I don't think that the dialogue to date has been broad enough. Public Safety Broadband also provides the opportunity for public safety to implement a *terrestria*l network, linking PSAPs, EOCs, and critical infrastructure facilities in a secure and reliable manner, free from the demands and limitations of the public internet. This network is necessary to support everything from VoIP communications, to GIS information, to Next Generation 911 routing. It would allow for the consolidation of PSAPs, the rerouting of volume around failures, the use of improved situational awareness tools, and the ability for the public safety community to depend on data communications unlike ever before. In short, it could change the entire landscape of the discipline.

The challenge lies in making all of this a reality in the current fiscal environment. As noted above, the Commonwealth's (and many other states) public safety communications budgets are stretched to the breaking point. After conducting an informal poll with the localities within Virginia, in which we asked how much they could afford to contribute towards the operation of a Public Safety Broadband network, the almost universal response is "if it cost more than my cellular service costs now, we can't do it". Virginia is made up of 135 jurisdictions, each with its own sense of budgetary priorities and fiscal demands. Since Virginia is a Commonwealth, each one of those 135 jurisdictions is also sovereign. This governance model is replicated in some form or fashion across the country, and in over eleven plus years of focusing on interoperability programs, what we've learned is that establishing mutually beneficial partnerships with the coalition of the willing that respects jurisdictional independence is a successful model for implementing interoperability programs. The existing Statewide Interoperability Executive Committees have been the laboratories for this approach, and their success is evidenced by their existence in every single state in the Union.

While no one can argue the need for broadband, the implementation of it has been the subject of much debate. It is only through a *partnership* between the states and localities, their existing governance structures, and the recently appointed "Firstnet" board that the program will be successful. In this context, the fact that there is not a single current state employee included in the recently announced First Net board appointments is of concern.

FirstNet, with all the best intentions in the world, cannot be expected to understand each states unique circumstances and needs. That is why national interoperability should be the task they focus on. There is a real urgency in many states to get communications resources up and running as soon as possible. As such, states should be allowed to proceed immediately with their plans, as long as they are interoperable with the nationwide network and meet minimum technical standards, and build their networks ahead of FirstNet . This is also true of all major cities, but especially true of Washington DC. This can be allowed under the "special consideration...to areas with unique homeland security requirements". Major cities typically represent the greatest threat from a terrorism and homeland security perspective and therefore need to have their communications networks up and running as a matter of priority.

Congress should recognize that the assigned spectrum has real value to states for their public safety communications mission and as a revenue generator. This revenue should flow straight to the states to fund their respective public safety communications missions, and an arrangement met for states to contribute from any surplus revenue to a FirstNet fund for the national interoperability mission. This should be the result of partnership between the individual states and FirstNet ,where states operate within a framework developed by FirstNet, but create partnerships with its jurisdictions and surrounding states to create coalitions of the willing that are able to work together to solve the myriad of implementation issues, at the correct geo-political level. States must also be allowed, within the interoperable requirements established by FirstNet, to pursue every technical means available, including those cited in the Presidents Panel report, to ensure that the spectrum is used as efficiently and effectively as possible. They must also be allowed to follow their codified procurement procedures that are designed to ensure that competition between vendors is maximized, resulting in reduced cost. The conversation surrounding broadband governance must not be allowed to devolve into an increasingly polarized discussion surrounding the "opt-in vs. opt-out" issue, usually driven by those without experience in managing the competing interests of local, state, and federal communications stakeholders.

Congress should be aware that even though the opt-out provision is in legislation, it seems that there has been an active effort to 'discourage' it. This risks interfering with the will of Congress. This is manifest in a number of ways, some subtle, some more blatant, and serves only to increase the tension of the conversation. "Opting out" is an explicit states right, as in the end they cannot and will not be forced to participate in a costly program that obligates state funds, should they choose not to. In many cases, "opting out" is a local right as well. In order to be successful in achieving our combined goal of a nationwide interoperable broadband capability for public safety, a successful model must be developed that falls somewhere in between the extremes "opt in vs. opt out", focusing on a sense of cooperation and problem solving that can result in an evolutionary leap forward in communications capabilities while providing adequate fiscal protection for its participants. Any other approach threatens alienating critical partners and fails to take into consideration each jurisdiction's unique and specific needs, potentially resulting in that jurisdiction being forced to "opt out", the very scenario we all wish to avoid.

Given recent events, it would be both irresponsible and inadvisable for the Commonwealth, or any other state, to enter into a project as expensive, far reaching, and mission critical as Public Safety Broadband without having adequate funding mechanisms in place to guard against the assumption of the availability of federal funding in perpetuity. We must, up front, ensure that the business model is in place that permits the network, its operation and maintenance, and the planning, training, and exercising that are going to be necessary to efficiently use it to be adequately and reliably funded.

This is not a simple or easy path, but Virginia is committed to this course because we strongly believe this "convergence" of voice and data communications is the future. Given the current budget environment, we also believe it is important that Federal, State, and local efforts are in alignment, working together efficiently towards a common goal. We are watching carefully the direction that FirstNet and other federally supported efforts are taking, hoping to assist them in a spirit of cooperation and openness. In this we can use your help. You can help us by putting the safeguards in place to make certain that these efforts are driven by the needs of states and localities, as well as making certain that the funding that you provide helps us to achieve those crucial goals. We look forward to working with you on these efforts.